UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

JANE DOE 1, and JANE DOE 2,
Plaintiffs,
vs.

MATTHEW WEISS; the REGENTS OF THE UNIVERSITY OF MICHIGAN; the UNIVERSITY OF MICHIGAN; KEFFER DEVELOPMENT SERVICES, LLC,

Defendants.

Case No. 25-CV-10806
Hon. Mark A. Goldsmith
Mag. Elizabeth A. Stafford

MOTION FOR AFFIRMATIVE INJUNCTIVE RELIEF

The purpose of this Motion is to permit Plaintiffs to learn the details of their victimization. Defendants know that detail. Plaintiffs do not.

Plaintiffs need to know for themselves, to protect themselves. Defendants and the federal government have confirmed Plaintiffs are victims. But Defendants refuse to provide any specific information about how they know as much, what their investigation(s) revealed, and the depth of the injuries that Plaintiffs have felt and will face, past and prospective.

Plaintiffs deserve to be able to rest assured and sleep at night knowing they have mitigated their harm to the extent possible. They have a right to know what

they can do realistically to contain the proliferation of their private, personal, identifying, and health information, not to mention whether and how far other, intimate information has traveled.

For these reasons, Plaintiffs, Jane Doe 1 and Jane Doe 2 ("Plaintiffs"), respectfully request entry of an Order granting them affirmative preliminary injunctive relief is against The Regents of the University of Michigan (the "Regents"), The University of Michigan (the "University"), Weiss, and Keffer Development Services, LLC ("Keffer").

Plaintiffs rely on their accompanying brief in support.

Date: April 15, 2025

Respectfully Submitted,

By: /s/*Parker Stinar*
Parker Stinar
Michael Grieco
Bryce Hensley *(admission pending)*
STINAR GOULD GRIECO & HENSLEY, PLLC
101 N. Wacker Dr., Floor M, Suite 100
Chicago, Illinois 60606
T: (312) 728-7444
parker@sgghlaw.com
mike@sgghlaw.com
bryce@sgghlaw.com

By: /s/*Patrick Lannen*
Patrick Lannen
Erik Johnson
STINAR GOULD GRIECO & HENSLEY, PLLC
550W. Merrill Street, Suite 249
Birmingham, Michigan 48009

patrick@sgghlaw.com
(269) 370-1746
erik@sgghlaw.com
(248) 221-8561

Counsel for Plaintiffs

By: */s/ Brian Glasser*
Brian A. Glasser (*admission pending*)
BAILEY & GLASSER LLP
1055 Thomas Jefferson Street,
NW, Suite 540
Washington, DC 20007
Phone: (202) 463-2101
bglasser@baileyglasser.com

By: */s/ Bart Cohen*
Bart D. Cohen
BAILEY & GLASSER LLP
1622 Locust Street
Philadelphia, PA 19103
Phone: (267) 973-4855
bcohen@baileyglasser.com

By: */s/ David Selby, II*
David L. Selby, II *(admission pending)*
BAILEY & GLASSER LLP
3000 Riverchase Galleria, Suite 905
Birmingham AL 35244
Phone: (205) 628-7575
dselby@baileyglasser.com

By: */s/ D. Todd Mathews*
D. Todd Mathews
BAILEY & GLASSER LLP
210 W. Division Street
Maryville IL 62062
Phone: (618) 418-5180
tmathews@baileyglasser.com

By: */s/ John W. Barrett*
John W. Barrett
Katherine E. Charonko (*admission pending)*
BAILEY & GLASSER LLP
209 Capitol Street
Charleston, WV 25301
Phone: (304) 345-6555
jbarrett@baileyglasser.com
kcharonko@baileyglasser.com
Counsel for Plaintiffs

By: /s/ *Aimee H. Wagstaff*
Aimee H. Wagstaff (admission pending)
Benjamin Gillig (admission pending)
WAGSTAFF LAW FIRM
940 N. Lincoln Street
Denver, CO 80203
Tel: 303-376-6360
awagstaff@wagstafflawfirm.com
bgillig@wagstafflawfirm.com

Counsel for Plaintiffs

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

JANE DOE 1, and JANE DOE 2,
Plaintiffs,
vs.

MATTHEW WEISS; the REGENTS OF THE UNIVERSITY OF MICHIGAN; the UNIVERSITY OF MICHIGAN; KEFFER DEVELOPMENT SERVICES, LLC,

Defendants.

Case No. 25-CV-10806
Hon. Mark A. Goldsmith
Mag. Elizabeth A. Stafford

BRIEF IN SUPPORT OF MOTION FOR AFFIRMATIVE INJUNCTIVE RELIEF

STATEMENT OF THE QUESTION PRESENTED

I. Plaintiffs have been identified as victims by both Defendants and by state and federal authorities following a completed police, and criminal investigation. Yet, Defendants refuse to provide any details about what their investigation revealed, and Plaintiffs do not know what specific actions they can or may wish to take to mitigate the harms and prevent further disclosure of their personal, private identifying, health, and any other information. Should the Court grant affirmative preliminary injunctive relief and require Defendants to provide specific details to Plaintiffs about what their investigation revealed, how they know Plaintiffs are victims, and provide details of all information known about what harm Plaintiffs have incurred and still will face?

Plaintiffs answer: "Yes."

The University and the Regents answer: "No."

The other Defendants are expected to answer: "No."

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

I. INTRODUCTION

Plaintiffs request entry of an Order requiring the defendants to provide specific detail about what their investigation into Plaintiffs' victimization revealed, what information confirms Plaintiffs are "victims," and the known extent of Plaintiffs' harm. Plaintiffs request this information for the pendency of this case so they can take any available action to prevent further harm and to go to bed at night understanding whether they are currently being, or likely to be, further victimized.

II. STATEMENT OF FACTS

A. Plaintiffs are Victims But Do Not Know the Extent of It.

The University and the Regents have apologized and offered identify theft protection. ECF No. 15–6, PageID.190–91. But they will not tell Plaintiffs any details about the "flaw" (the "**Flaw**") in their computer network that compromised Plaintiff's private data. *Id.* at PageID.188.

The Department of Justice has corroborated that Plaintiffs are "victims." ECF No. 15–7, PageID.195. The victimization extends to aggravated identify theft, and includes "thousands of candid, intimate photographs and videos" with "many" including "victims engaged in explicit sexual acts." *Id.* The specific details of methods taken to victimize Plaintiffs, when, through what medium, by who (all such actors), and what was taken, lost, and what can or will happen, however, is never provided.

B. This Is Not the First Cyber Attack.

The University has had other cybersecurity breaches. In this case, it is undisputed that the University has known since at least December 2022 that there had been a significant data breach of student athlete personally identifiable information ("PII"), including candid and intimate images. Since that time, there have been other, repeat data security breaches at the University.

The 2022 breach did not come to light until March 20, 2025. It was then that the Government charged Defendant Matthew Weiss ("Weiss") with a 24-count indictment alleging 14 counts of unauthorized access to computers and 10 counts of aggravated identity theft.

In August 2023, hackers gained access to up to 230,000 individuals including the PII of students and applicants, alumni and donors, employees and contractors, University Health Service and School of Dentistry patients, and research study participants. The University later informed individuals whose information was likely stolen and offered free credit monitoring services.[1] In September 2024, Michigan Medicine had a *second* cyberattack in four months targeting employee email accounts and compromising protected health information, such as the names,

[1] *See* https://www.detroitnews.com/story/news/local/michigan/2023/10/23/um-3rd-party-accessed-school-systems-personal-information-for-5-days/71292044007/ (last visited on April 13, 2025).

medical record numbers and diagnostic and/or treatment information of nearly 58,000 people.[2]

When these latter two major cybersecurity attacks occurred, the University and the Regents knew of the prior major security breach at issue here and knew so by at least December 2022. *See* **Exhibit A**–name redacted.

But for reasons that remain unknown, Plaintiffs-victims were never told their student athlete information had been compromised. *Id.* Between January 10 and February 2, 2023, the 15th District Court in Ann Arbor signed at least 14 search warrants, giving investigators permission to seize items from the home and office of Weiss, as well as the quarterback and tight end meeting rooms at Schembechler Hall and the campus Administrative Services Building.[3] The partial extent of that data breach did not come to light until March 2025 when the Government indicted Weiss.

Again, in all of this time, extended harm to Plaintiffs could have been avoided.

C. The "Flaw" Letter.

By letter sent in March 2023, the University delivered notice to Plaintiff that the "**Flaw**" in its computer network compromised Plaintiff's private data. **Exhibit**

---

[2] *See* https://www.freep.com/story/news/health/2024/09/26/cybersecurity-breach-university-of-michigan-medicine-email-attack/75392949007/ (last visited on April 13, 2025).

[3] *See* https://www.detroitnews.com/story/news/local/michigan/2025/03/26/warrants-reveal-what-was-seized-from-ex-um-coach-weiss-home-office/82678503007/ (last visited on April 13, 2025).

A. The letter describes itself as a "follow-up" to an "investigation" *by* the "University of Michigan Police Department." *Id.* at 1. In the preamble, the letter offers to provide Plaintiff "some additional information, as well as offer you identity theft protection coverage." *Id.*

1. "Additional Information -- the "What happened" Section.

In the first section, titled "What happened," the University explains it "identified" "in late December 2022, potentially unauthorized activity in your U-M Google account." *Id.* As part of its "investigation," the University "discovered that a 'threat actor' manipulated a ***flaw*** in [the U-M Google account] self-service password-recovery to change your password and gain unauthorized access to your U-M Google account." *Id.* The letter defines the self-service recovery function as "Forgot password." *Id.*

Plaintiffs did not know at the time that the "threat actor" was Weiss, then a high paid employee of the University. Evidently, "these findings were escalated" to "University police, which subsequently launched a criminal investigation." *Id.*

Based on its investigation, the University next states, the ***Flaw*** in Forgot password is what permitted the "threat actor" to "gain[] unauthorized access to some of your accounts and/or data." *Id.* While the University did not further identify or describe the Flaw, it explained that, because of the Flaw, the "threat actor" "also logged into your U-M account management settings, where 'they' may have viewed

and/or changed your password recovery phone number and password recovery email address." *Id.* In the same paragraph, the letter definitively states that "[a]dditionally, 'they' logged into your M+ Google email and/or Google Drive." *Id.* However, the University "cybersecurity team was unable to tell which emails or files 'they' may have accessed or deleted while logged in, or whether your email settings were altered. *Id.*

The letter confirms that personal information *was* accessed. The letter states, "law enforcement investigations have determined 'they' [referring to the 'threat actor'] were able to use information in your account to access additional personal information, which may include access details for accounts inked to your U-M email address (online banking, social media, password management, etc.)" *Id.*

In sum, while written in past tense and defensive in tone, the letter discloses without qualification that it was the University's technology ***flaw*** that permitted one of its own employees to access without authorization Plaintiff's personal online banking, social media, and password management data.

2. The "What we are doing about this" section.

The next section of the letter states that, "as part of the response and investigation," the University took certain actions including that it:

- Randomized your password, so the 'threat actor' would no longer be able to access your account;
- Identified and fixed the flaw in the password reset application;

- Engaged University police so they could pursue a criminal investigation;
- Continue[s] to support the University policy and other U-M 'inquiries' into the "matter."

Id.

No other detail about how the flaw came to exit, what exactly it is, or how it was used is more specifically described, though the University claimed it was "fixed." *Id.* Nor were any other details about the "investigation" revealed. *Id.*

3. The "What you should do" section.

Next, the letter directed Plaintiff to reset her password, if she had not already done so, after December 23, 2022. *Id.* The letter also provided a phone number for technology support. *Id.* It provided advice to enable a "two-factor authentication" feature and a "security check up." *Id.* at 2. However, no reason was given why this advice was not previously provided.

4. The "U-M provided identify theft protection" section.

In the next section, the University suggested that Plaintiff remain vigilant of fraud and identity theft. *Id.* The University offered one-year complimentary "LifeLock Standard™ identity theft protection" and described features that it believed that protection offered. *Id.*

5. The "additional identity theft guidance" section.

The letter next included three "identity theft subsections," including "account credit monitoring," "consider a credit freeze," and "report identity theft." *Id.* at 3. In

the first subsection, the letter identified the three major credit bureaus and suggested each has a free service for further fraud alert protection. *Id.* In the next, the letter suggested that a "credit or security 'freeze'" would permit Plaintiff to "restricts access" to her credit report, "which makes it more difficult for identify thieves to open new accounts in your name." *Id.* Finally, the letter suggested reporting identify theft if Plaintiff believed she was a victim. *Id.*

6. The "Find out more about securing your devices and accounts" section.

The letter next identified three websites for Plaintiff to help her protect herself. *Id.* at 4. It also identified a website of the University information technology service department. *Id.*

7. The "We apologize for this issue" section.

The letter concluded by acknowledging "how important your personal information is" and that the University "deeply regret[s] that this situation occurred." *Id.* The University stated it "is committed to maintaining a secure computing environment, preserving the confidentiality of the information we maintain, and constantly reviewing and improving our security practice." *Id.*

The University apologized "for any inconvenience this incident has caused you" and offered the email address privacy@umich.edu and a local phone number, with the phrase "Data Incident Notification Letter from Feb. 2023," as a resource to "talk to someone about this situation." *Id.*

The letter was signed by Sol Bermann, the Chief Information Security Officer, Executive Director of Information Assurance for the University. *Id.*

D. The Mega Victim Case Assistance Program (MCAP) Email.

By email dated March 27, 2025, Plaintiff Doe 2 contacted the Department of Justice because she received an email confirming she was a victim of the "incident" described in **Exhibit A**. *See* **Exhibit B**—name redacted. That same day, the Mega Victim Case Assistance Program ("MCAP") of the United States Attorney's Office returned Plaintiff's email and stated that Plaintiff was, in fact, "a victim of unauthorized access and aggravated identity theft." The email states that "the defendant" "gained unauthorized access to the email, social media, and cloud storage accounts of 2000+ victims between 2015 and 2023." *Id.*

The email states that "[t]housands of candid, intimate photographs and videos have been seized from the [criminal] defendant's electronic storage devices and his cloud storage accounts." *Id.* The email specifies that "[m]any" of the photographs and images "show victims naked" and that "[s]ome show victims engaged in explicit sexual acts." *Id.*

The email indicates that there is an active FBI investigation ongoing. The email recommends resetting passwords across online accounts, especially those containing "sensitive information," including but not limited to financial accounts, email accounts, file storage accounts, and social media accounts. *Id.* The email

strongly advises against reusing passwords and endorses "additional" levels of electronic authentication. Finally, the email offers resources for further identify theft information about safe practices. *Id.*

III. PROCEDURAL POSTURE

On Friday, March 21, 2025, Plaintiffs filed this putative class action case. ECF No. 1. It was the first filed but there are a number substantially similar cases, Case Nos. 10855, 10870, 10876, 10946, 10951, 10988, 10999. The Complaint asserts Plaintiff Doe 1 was a student athlete at the University between 2017 and 2018 and was a member of the Women's Gymnastics team. *Id.* ¶ 1. It explains Plaintiff Jane Doe 2 was a student athlete at the University between 2017 and 2023 and was a member of the Women's Soccer team. *Id.* ¶ 3.

In sum and substance part, the Complaint alleges Weiss was employed by the University, and that the Regents and the University failed in duties to supervise and monitor Weiss in a manner that would not result in a breach of their privacy and to which they entrusted to the University. *Id.* ¶¶ 13, 18, and 19. Plaintiffs allege they entrusted the University to safeguard their information. *Id.* ¶ 29. Plaintiffs allege the University therefore had a heightened duty and breached it by failing to safeguard the computer network against Weiss being able to use his University electronic credentials and University provided intellectual and physical property to access their information, images, and videos. *Id.* ¶¶ 30, 35, 37, 91.

Similar allegations are made against Keffer, a technology company that the University authorized to be in contact with Weiss and to do so in connection with student athlete services including for athletic training. *Id.* ¶¶ 41, 44, 45. Class allegations are made based on the public reports from the United States Attorney's Office and others, including the University, that the unauthorized access by Weiss as a result of the Flaw affected thousands of victims. *Id.* ¶¶ 55. The Complaint alleges a failure to properly supervise and employ Weiss against all non-Weiss defendants and includes various assertions of gross negligence and recklessness in this respect. *Id.* ¶¶ 57–59, 63–72, 80–83.

It appears uncontested that thousands of other victims and absent class members were harmed in the same manner and by the same means as Plaintiffs. ECF No. 1, ¶¶ 109–122. Plaintiffs understand it is not disputed that Weiss was an employee or that he accessed personal information of many victims including Plaintiffs while a University employee and a result of information and electronic credentials provided to him as a result of that employment. Allegations of this ilk are throughout the Complaint including in paragraphs 77–79, 109–122.

The Complaint currently includes fifteen claims: (1) Violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (Count I, and alleging Weiss was an "insider hacker" because he accessed a computer with permission that dealt with Plaintiffs and other class members, but that Weiss exceeded the parameters of

authorized access); (2) Violation of the Stored Communication Act, 18 U.S.C. § 2701 *et seq.* (Count II); (3) Violation of Title IX, 20 U.S.C. § 1681 *et seq.*, focusing on the more pervasive effects of the misconduct as victimizing women (Count III); (4) Violation of 42 U.S.C. § 1983 for State Created Danger (Count IV); (5) Violation of 42 U.S.C. § 1983 for Failure to Train and Supervise (Count V); (6) Invasion of Privacy Intrusion Upon Seclusion (Count VI); (7) gross negligence (Count VII); (8) negligent hiring (Count VIII); (9) negligent training (Count IX); (10) negligent supervision (Count X); (11) negligent entrustment (Count XI); negligent retention (Count XII); Trespass to Chattels (Count XIII); common law conversion (Count XIV); statutory conversion under Mich. Comp. Laws § 600.2919a (Count XV).

The Complaints in the other actions are substantially similar. In the one other motion filed, from Case No. 10855, at ECF 15-2, PageID.158, the plaintiffs used, literally, the exact exhibits from *this case* (Case No. 10806), from the Motion for Expedited Discovery (ECF No. 15) as evidence of apparently their claims, though that is evidence only from the Plaintiffs to this case.

IV. PRELIMINARY INJUNCTION

"A preliminary injunction is an extraordinary remedy never awarded as of right." *Winter v. Nat. Res. Def. Council, Inc.*, 555 U.S. 7, 24 (2008) (citation omitted). "A plaintiff seeking a preliminary injunction must establish that he is likely to succeed on the merits, that he is likely to suffer irreparable harm in the absence of

preliminary relief, that the balance of equities tips in his favor, and that an injunction is in the public interest." *Id.* at 20. In each case, courts "must balance the competing claims of injury and must consider the effect on each party of the granting or withholding of the requested relief." *Id.* at 24, (quoting *Amoco Prod. Co. v. Vill. of Gambell, AK*, 480 U.S. 531, 542 (1987)).

"When considering a motion for a preliminary injunction, the district court should consider four factors: (1) whether the movant has a strong likelihood of success on the merits; (2) whether the movant would suffer irreparable injury without the injunction; (3) whether issuance of the injunction would cause substantial harm to others; and (4) whether the public interest would be served by issuance of the injunction." *Rock and Roll Hall of Fame and Museum, Inc. v. Gentile Productions*, 134 F.3d 749, 753 (6th Cir. 1998). A district court must make specific findings concerning each of these factors, unless analysis of fewer facts is dispositive of the issue. *Six Clinics Holding Corp., II v. Cafcomp Systems, Inc.*, 119 F.3d 393, 399 (6th Cir. 1997). However, not all the factors need to be fully established for an injunction to be proper. *Michigan State AFL-CIO v. Miller*, 103 F.3d 1240, 1249 (6th Cir. 1997). None is a prerequisite to relief; rather, they should be balanced. *Connection Distributing Co. v. Reno*, 154 F.3d 281, 288 (6th Cir. 1998).

As the Supreme Court has explained, the purpose of a preliminary injunction "is merely to preserve the relative positions of the parties

until a trial on the merits can be held." *Univ. of Tex. v. Camenisch*, 451 U.S. 390, 395 (1981). Motions seeking to obtain affirmative preliminary injunctive relief must be more closely scrutinized than a motion for preliminary junction which seeks to maintain the status quo. *See, e.g., Russell v. Tribley*, 2011 WL 4387589, at *10 (E.D. Mich. Aug. 10, 2011), *report and recommendation adopted*, 2011 WL 4396784 (E.D. Mich. Sept. 21, 2011) (citing *Schrier v. Univ. of Colo.* 427 F.3d 1253, 1259 (10th Cir. 2005), and *Johnson v. Kay*, 860 F.2d 529, 540 (2d Cir. 1988)); *Doe v. Tennessee*, 2018 WL 5313087, at *4 (M.D. Tenn. Oct. 26, 2018), *report and recommendation adopted*, 2018 WL 6181349 (M.D. Tenn. Nov. 27, 2018).

The standard has been stated as requiring the injury be of "such imminence that there is a clear and present need" for relief in order to prevent harm. *See Wis. Gas Co. v. Fed. Energy Regulatory Comm'n*, 758 F.2d 669, 674 (D.C. Cir. 1985) (quotations omitted).

A. Likelihood of Success on the Merits

Plaintiffs are likely to succeed in most, if not all, of their claims. For example, Count I alleges violations of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, *et seq*. Weiss violated the Act because he "intentionally accesse[d] a computer without authorization" and/or "exceed[ed] authorized access, and thereby obtain[ed] ... information." 18 U.S.C. § 1030(a)(2)(C). The University is vicariously liable for Weiss's actions because Weiss did so in furtherance of his role as a medical sports

employee of the University's athletic department. The University is vicariously liable for any completed offenses of its agents. *See Abu v. Dickson*, 107 F.4th 508, 514 (6th Cir. 2024) (citing *Meyer v. Holley*, 537 U.S. 280, 285 (2003)).

Additionally, the University's, the Regents' (and Keffer's) gross negligence in failing to consider, implement, or follow a policy to oversee how or whether the University (and Keffer) conducted its operations in a manner that would have monitored, supervised, and ensured that retention and employment of Weiss would not result in a breach of Plaintiffs' privacy is an indefensible claim. The same facts support the fact that the University failed to train and supervise Weiss, which showed a deliberate indifference to the well-being of Plaintiffs and the putative class. Similar facts support Plaintiffs' negligent hiring claim, negligent training claim, negligent supervision claim, and negligent entrustment claim.[4]

B. Irreparable Harm

A plaintiff's harm from the denial of a preliminary injunction is irreparable if it is not fully compensable by monetary damages. *Basicomputer Corp. v. Scott,* 973 F.2d 507, 511 (6th Cir. 1992). *McDonell v. Hunter,* 746 F.2d 785, 787 (8th Cir. 1984) (finding that a violation of privacy constitutes an irreparable harm). Other Circuits have developed a three-factor test to determine "when the risk of future

[4] Additionally, at common law, invasion of the right to privacy is a tort. The species at issue here, Intrusion upon Plaintiffs seclusion or solitude, is a claim for which there is no real dispute that Plaintiffs' privacy rights have been violated. Restatement (Second) of Torts, § 652A (1977).

misuse of PII following a data breach is imminent and substantial." *Webb v. Injured Workers Pharmacy, LLC*, 72 F.4th 365, 375 (1st Cir. 2023). Those three factors include the following:

1. whether the plaintiffs' data has been exposed as the result of a targeted attempt to obtain the data;

2. whether any portion of the dataset has already been misused, even if the plaintiffs themselves have not yet experienced identity theft or fraud; and

3. whether the type of data that has been exposed is sensitive such that there is a high risk of identity theft or fraud.

McMorris v. Carlos Lopez & Assocs., LLC, 995 F.3d 295, 301, 303–05 (2d Cir. 2021). These factors are not necessarily exclusive. *Id.* And, in the First Circuit's view, they are not "necessarily determinative[.]" *Webb*, 72 F.4th at 375. "[B]ut they do provide guidance." *Id.*[5] Here, each of the factors is met.

1. Plaintiffs' data has been exposed as the result of Weiss's attempt to obtain Plaintiffs' PII and the other Defendants' failure to protect the information.

[5] The Supreme Court has recognized that some of its cases may indicate the existence of an individual privacy interest in avoiding disclosure of personal matters. *Whalen v. Roe,* 429 U.S. 589 (1977). The *Whalen* Court observed that "the cases sometimes characterized as protecting 'privacy' have ... involved ... the individual interest in avoiding disclosure of personal matters." *Id.* at 598–99; *see also Nixon v. Adm'r of Gen. Servs.,* 433 U.S. 425, 457 (1977) (citing *Whalen* and finding that public officials may have a privacy interest in avoiding disclosure of personal matters that are unrelated to the acts they perform in their official capacities).

There is no question that Plaintiffs' PII has been exposed by a targeted effort to obtain the information. "It stands to reason that data compromised in a targeted attack is more likely to be misused." *Web*, 72 F.4th at 375. It is not currently known what Weiss has done or intended to do with Plaintiffs' PII. The breadth of the data breach raises many questions. The most shocking revelation is of course that Weiss obtained Plaintiffs' personal and intimate photographs. But why? Was it for personal gratification, extortion, other financial gain? It is not clear. Plaintiffs deserve to know.

It is also not clear why he obtained Plaintiffs' protected health information ("PHI"), email passwords, and Keffer-stored athlete data. That kind of information does not readily lend itself to the theory that Weiss is only a sexual predator. What else Weiss intended to do with the information cannot be divined by what little information released by the Government and the Defendants here.

The first factor is easily met where at the very least, Plaintiffs' PII and PHI have been exposed to Weiss, and potentially more.

2. Plaintiffs' PII has already been misused.

Weiss's use of Plaintiffs' PII alone is misuse. Weiss gathered Plaintiffs' PII and PHI, along with the putative class's information, for years. "[T]he risk of future misuse may be heightened where the compromised data is particularly sensitive." *Id*. at 376. "Naturally, the dissemination of high-risk information such as Social

Security numbers and dates of birth -- especially when accompanied by victims' names -- makes it more likely that those victims will be subject to future identity theft or fraud." *Id*.

Here, in addition to the highly detailed PII obtained by Weiss, personal and intimate photos and videos were stolen by Weiss. How Plaintiffs' PII, PHI, and personal and intimate images were used is unknown at this time. Did Weiss do more than use the voluminous information he stole for personal gratification? It seems reasonably likely that he sold some of the information or used it for some other form of financial gain. There is no question that the Plaintiffs' PII and PHI have been misused at least by Weiss. But there is at least reason to believe that the information has been received and obtained by others. *See id.* at 376 (reasoning "that at least some information stolen in a data breach has already been misused also makes it likely that other portions of the stolen data will be similarly misused").

3. Plaintiffs' PII is sensitive such that there is a high risk of identity theft or fraud.

Plaintiffs' PII and PHI are sensitive such that there is a high risk of identity theft. Courts have recognized that information such as social security numbers and birth dates, especially when accompanied by a victim's name, is sensitive information making misuse of the information a high risk. *McMorris v. Carlos Lopez & Assocs., LLC*, 995 F.3d 295, 302 (2d Cir. 2021). This is true "even if that misuse has not yet resulted in an actual or attempted identity theft." *Id.* That some of the

information has been misused, as it has here, supports "a finding that those plaintiffs are at a substantial risk of identity theft or fraud." *Id.*

Here, Plaintiffs have loss control of their PII, PHI, and personal and intimate images and an accompanying impairment in the value of that information. *See Smith v. Findlay Automotive*, 2025 WL 973859, at *3 (D. Nev. Mar. 31, 2025) (finding compensable injury arising from the loss of control of the plaintiffs' identities and the accompanying impairment in value of their PII). Plaintiffs' information has been misused by Weiss, and likely others. That risk continues until Plaintiffs' information is secured and the depth of the dissemination of their information is better known.

Plaintiffs will suffer irreparable harm without a preliminary injunction. In *Bosley v. Wildwett.com*, the defendant took an unauthorized video of the plaintiff, who was a local newscaster, while she was unclothed during a wet t-shirt contest. 310 F. Supp. 2d 914, 917 (N.D. Ohio 2004). As the court explained, "without a preliminary injunction, it may become impossible for Plaintiff to minimize lasting damages to her persona." *Id*. at 934. The court explained that "the sooner [the plaintiff] is able to regain control of her persona, the more likely she is to be able to turn around her career. *Id*.

Here, a preliminary injunction is necessary to prevent immediate and irreparable loss to Plaintiffs, including the potential dissemination of personal and intimate images, PII, and PHI. Plaintiffs and the putative class members have

suffered a significant and compensable injury arising from the loss of control of their identity and the accompanying impairment in value of their PII. *See Smallman v. MGM Resorts Int'l*, 638 F. Supp. 3d 1175, 1188 (D. Nev. 2022) (collecting cases within the Ninth Circuit finding that an individual's loss of control over PII constitutes a cognizable harm); *see also Pruchnicki v. Envision Healthcare Corp*., 439 F. Supp. 3d 1226, 1234 (D. Nev. 2020), *aff'd*, 845 Fed. Appx. 613 (9th Cir. 2021) (finding diminution in the value of personal information can be a viable theory of damages in a data breach case). Therefore, Plaintiffs will be irreparably harmed if no injunctive relief is granted.

C. There is No Substantial Harm to Defendants.

Defendants will not be subject to substantial harm if the Court issues a preliminary injunction. Plaintiffs are seeking to secure their PII and PHI currently in the University's and Keffer's possession, and to learn how much of their information has been disseminated, to whom, and for how long. Defendants already have an obligation to protect Plaintiffs' information in the University's and Keffer's possession. For years, however, they have repeatedly failed to do so, as evidenced by repeated major data breaches over the last three years. Plaintiffs request a preliminary injunction, in part, requiring that the University and Keffer disclose the extent of the investigation and what it has revealed.

That will cost the Defendants nothing. They say they have already implemented adequate security protocols consistent with industry standards. So why not tell Plaintiffs? To protect themselves, Plaintiffs are entitled to know how and where they were victimized, including for the purpose of knowing whether they are likely to suffer further harm. What information or limitation of harm is known? What more is needed? Are there ongoing programs (and what are they) to prevent further harm, and do they include encryption, regular audits, and employee training, to prevent future data breaches that would further victimize Plaintiffs?

Plaintiffs seek to know the depth of Weiss's activities to better understand how Plaintiffs can protect themselves from any further harm. The University and Keffer have both conducted investigations into the matter. Plaintiffs seek an affirmative preliminary injunction requiring that the information learned during those respective investigations and what they revealed be shared, at least confidentially, so that Plaintiffs can evaluate for themselves what actions they will take to protect themselves from further victimization.

D. The Relief Requested is in the Public Interest.

The public interest is best served by a preliminary injunction protecting Plaintiffs' privacy rights. The informational-privacy interest in this case has a constitutional dimension. *See Lee v. City of Columbus, Ohio*, 636 F.3d 245, 260 (6th Cir. 2011) (explaining that the Sixth Circuit has "recognized an informational-

privacy interest of constitutional dimension in only two instances: (1) where the release of personal information could lead to bodily harm (*Kallstrom*), and (2) where the information released was of a sexual, personal, and humiliating nature (*Bloch*)"); *see also Nixon v. Adm'r of Gen. Servs*., 433 U.S. 425, 457 (1977) (noting that the right to privacy includes an "'individual interest in avoiding disclosure of personal matters'"). "Our sexuality and choices about sex . . . are interests of an intimate nature which define significant portions of our personhood." *Bloch v. Ribar*, 156 F.3d 673, 685 (6th Cir. 1998). "Publicly revealing information regarding these interests exposes an aspect of our lives that we regard as highly personal and private." *Id*. The public has a strong interest in seeing Plaintiffs' private and intimate information protected.

Both the public and the University should be aligned in preventing any further data breaches exposing Plaintiffs PII at the University. And allowing the victims whose PII, PHI, and intimate and personal images were stolen to know to what extent their information has been compromised gives them some control of their information, which clearly benefits the public interest in privacy. This matter, above all others, is perhaps the most important.

E. No Bond Should Be Required.

Federal Rule of Civil Procedure 65(c) requires a preliminary injunction applicant to post a bond "in such sum as the court deems proper, for the payment of

such costs and damages as may be incurred or suffered by any party who is found to have been wrongfully enjoined or restrained." The security requirement of Rule 65(c) informs the applicant "the price it can expect to pay if the injunction was wrongfully issued." *Sprint Communications Co. v. Cat Communications Int'l*, 335 F.3d 235, 240 (3d Cir. 2003) (quoting *Instant Air Freight Co. v. C.F. Air Freight, Inc*., 882 F.2d 797, 805 (3d Cir. 1989)).

While the language of Rule 65(c) appears to be mandatory, "the rule in our circuit has long been that the district court possesses discretion over whether to require the posting of security." *Moltan Co. v. Eagle–Picher Indus., Inc*., 55 F.3d 1171, 1176 (6th Cir. 1995) (citing *Roth v. Bank of the Commonwealth*, 583 F.2d 527, 539 (6th Cir. 1978)). For example, the Sixth Circuit has upheld a district court's waiver of a bond requirement where the district court determined that the plaintiff had a strong case, backed by strong public interest. *Id*.

Here, Plaintiffs are willing to post bond, but based upon the merits of their case and the irreparable harm that will occur without a preliminary injunction, they request that the Court not require them to post bond.

V. CONCLUSION

The University has had multiple major data security breaches in the last three years and there is no dispute that Plaintiffs' PII, PHI, and personal and intimate images have been misused. Plaintiffs are victims. Defendants should be ordered to

disclose the details of that victimization so that Plaintiffs can further protect themselves. Depriving victims of information is not helpful. Due to the University's repeated security breaches resulting in actual harm to Plaintiffs, Plaintiffs seek the following relief:

1. Ordering the University to disclose to Plaintiffs the details of (a) how it was learned that their personal, private information was accessed, (b) by who, (c) when, (d) what methods were used for that access, (e) what damage is believed to have occurred, (f) will occur, and (g) why no other damages are likely in the eyes of the Defendants;

2. Disclosing (a) what security protocols are now being used, (b) why, (c) whether and how they are consistent with industry standards, (d) including encryption, (e) regular audits, and (f) employee training, to prevent future data breaches that would impact Plaintiffs.

3. Ordering the University, the Regents, and Keffer, subject to a protective order, to immediately disclose the extent of their information gathered from their respective investigations into Weiss's actions so that Plaintiffs can determine what other protection or mitigating action they can take to reduce harm.

Date: April 15, 2025

Respectfully Submitted,

By: /s/*Parker Stinar*
Parker Stinar
Michael Grieco
Bryce Hensley *(admission pending)*

STINAR GOULD GRIECO & HENSLEY, PLLC
101 N. Wacker Dr., Floor M, Suite 100
Chicago, Illinois 60606
T: (312) 728-7444
parker@sgghlaw.com
mike@sgghlaw.com
bryce@sgghlaw.com

By: /s/*Patrick Lannen*
Patrick Lannen
Erik Johnson
STINAR GOULD GRIECO & HENSLEY, PLLC
550W. Merrill Street, Suite 249
Birmingham, Michigan 48009
patrick@sgghlaw.com
(269) 370-1746
erik@sgghlaw.com
(248) 221-8561

Counsel for Plaintiffs

By: */s/ Brian Glasser*
Brian A. Glasser (*admission pending*)
BAILEY & GLASSER LLP
1055 Thomas Jefferson Street,
NW, Suite 540
Washington, DC 20007
Phone: (202) 463-2101
bglasser@baileyglasser.com

By: */s/ Bart Cohen*
Bart D. Cohen
BAILEY & GLASSER LLP
1622 Locust Street
Philadelphia, PA 19103
Phone: (267) 973-4855
bcohen@baileyglasser.com

By: */s/ David Selby, II*
David L. Selby, II *(admission pending)*
BAILEY & GLASSER LLP
3000 Riverchase Galleria, Suite 905
Birmingham AL 35244
Phone: (205) 628-7575
dselby@baileyglasser.com

By: */s/ D. Todd Mathews*
D. Todd Mathews
BAILEY & GLASSER LLP
210 W. Division Street
Maryville IL 62062
Phone: (618) 418-5180
tmathews@baileyglasser.com

By: */s/ John W. Barrett*
John W. Barrett
Katherine E. Charonko (*admission pending)*
BAILEY & GLASSER LLP
209 Capitol Street
Charleston, WV 25301
Phone: (304) 345-6555
jbarrett@baileyglasser.com
kcharonko@baileyglasser.com
Counsel for Plaintiffs

By: /s/ *Aimee H. Wagstaff*
Aimee H. Wagstaff (admission pending)
Benjamin Gillig (admission pending)
WAGSTAFF LAW FIRM
940 N. Lincoln Street
Denver, CO 80203
Tel: 303-376-6360
awagstaff@wagstafflawfirm.com
bgillig@wagstafflawfirm.com

Counsel for Plaintiffs

CERTIFICATE OF SERVICE

I hereby certify that on April 15, 2025, I electronically filed the foregoing Motion, Brief in Support and corresponding exhibits with the Clerk of the Court using the ECF system which will send notification of such filing to all parties registered.

s/*Parker Stinar*
Parker Stinar
STINAR GOULD GRIECO & HENSLEY, PLLC